Office of the Governor
State Chief Information Officer

SECURITY

Chapter 13 – Detecting and Responding to IS Incidents

Scope: These standards apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: G.S. §147-33.110; G.S. §147-33.113

Section 01 Reporting Information Security Incidents

130101 Reporting Information Security Incidents

Purpose: To increase effectiveness in assessing threat levels and detecting patterns or trends in regard to security incidents through proper documentation.

STANDARD

All information technology security incidents must be reported to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, and must include the information required on the Incident Reporting form,[1] incorporated by reference.

The agency head shall ensure that all information technology security incidents occurring within his/her agency are reported to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, within twenty-four (24) hours of incident confirmation.

GUIDELINES

Agencies shall report incidents to the ITS Information Security Office by:

- Contacting ITS Customer Support Center 800-722-3946
- Using the incident reporting website https://incident.its.state.nc.us
- Contacting a member of the ITS Information Security Office staff directly

[1] The Incident Reporting form can be found at https://incident.its.state.nc.us/ and can be filled out online.

Computer security incidents are divided into five levels of severity based on their potential to negatively impact North Carolina agency operations, finances, and/or public image. The characteristics in the table below are intended to serve as general guidelines only, and should not be interpreted as absolutes.

Incident Severity	Incident Characteristics
5 GENERAL ATTACK(S) **SEVERE**	▪ Successful penetration or denial-of-service attack(s) detected with significant impact on North Carolina ITS operations: o Very successful, difficult to control or counteract o Large number of systems compromised o Significant loss of confidential data o Loss of mission-critical systems or applications ▪ Significant risk of negative financial or public relations impact
4 LIMITED ATTACK(S) **HIGH**	▪ Penetration or denial-of-service attack(s) detected with limited impact on North Carolina ITS operations: o Minimally successful, easy to control or counteract o Small number of systems compromised o Little or no loss of confidential data o No loss of mission-critical systems or applications ▪ Widespread instances of a new computer virus or worm that cannot be handled by deployed anti-virus software ▪ Small risk of negative financial or public relations impact
3 SPECIFIC RISK OF ATTACH **ELEVATED**	▪ Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance ▪ Penetration or denial of service attack(s) attempted with no impact to North Carolina ITS operations ▪ Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software ▪ Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software
2 INCREASED RISK OF ATTACH **GUARDED**	▪ Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance ▪ Penetration or denial of service attack(s) attempted with no impact to North Carolina ITS operations ▪ Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software ▪ Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software
1 **LOW**	▪ Small numbers of system probes, scans, and similar activities detected on internal systems ▪ Isolated instances of known computer viruses or worms, easily handled by deployed anti-virus software

ISO 17799: 2005 References
13.1.1 Reporting information security events

130102 Reporting IS Incidents to Outside Authorities

Purpose: To ensure agency awareness of the State's authority to determine when confirmed security incidents should be reported to appropriate third parties.

STANDARD

The ITS Information Security Office, acting on behalf of the State Chief Information Officer, shall determine what, if any, outside authorities need to be contacted in regard to confirmed security incidents in accordance with applicable laws and procedures, any Memorandum of Understanding between ITS, the Department of Justice, the State Bureau of Investigation, and the Office of the State Auditor as well as in accordance with federal requirements.

ISO 17799: 2005 References
13.1.1 Reporting information security events

130103 Reporting Information Security Breaches

Purpose: To ensure that all confirmed information security breaches are reported.

STANDARD

The State's workforce has the responsibility to report security incidents to agency management in accordance with statewide standards and agency standards, policies, and procedures. Agency management has the responsibility to report security incidents to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, as required by N.C.G.S. §147-33.113 and in accordance with Standard 130101, Reporting Information Security Incidents, and Standard 130102, Reporting Information Security Incidents to Outside Authorities.

ISO 17799: 2005 References
13.1.1 Reporting information security events

130104 Notifying Information Security Weaknesses

Purpose: To reduce information technology security weaknesses.

STANDARD

All agency personnel have the responsibility to report any discovered security weaknesses to their agency management in accordance with state and agency standards, policies and procedures. The notification should be made as soon as possible after the weakness is discovered.

ISO 17799: 2005 References
13.1.2 Reporting security weaknesses

130105 Witnessing an Information Security Breach

Purpose: To protect the State's information technology assets.

STANDARD

Individuals who witness a breach in an agency's information technology security shall notify their management in accordance with state and agency standards, policies and procedures.

ISO 17799: 2005 References
13.1.1 Reporting information security events

130106 Being Alert for Fraudulent Activities

Purpose: To protect the State's resources.

STANDARD

Upon detection, suspected fraudulent activity shall be documented and reported to agency management in accordance with agency state and agency standards, policies and procedures for appropriate action as soon as possible.

ISO 17799: 2005 References
8.2.2 Information security awareness, education, and training

130107 Software Errors and Weaknesses

Purpose: To ensure proper handling of software errors and weaknesses.

STANDARD

Personnel who discover or perceive that there may be a software error or weakness must be report it immediately to agency management. Management shall notify the responsible individual/organization and perform a risk analysis of the perceived threats.

Individuals who are aware of software errors or weaknesses shall not attempt proof-of-concept actions unless otherwise authorized.

ISO 17799: 2005 References
13.1.2 Reporting security weaknesses

130108 When and How to Notify Authorities

Purpose: To ensure appropriate notification of authorities, regulatory and enforcement agencies about information security incidents.

STANDARD

Agencies shall notify the ITS Information Security Office of information security incidents. The ITS Information Security Office shall notify authorities, regulatory and law enforcement agencies about information security incidents in accordance with the State's Incident Management Plan.

If/when authorities, regulatory and/or law enforcement agencies are notified; agencies shall report the incident to the Incident Management team and/or the Chief Information Security Officer.

ISO 17799: 2005 References
6.1.6 Contact with authorities

Section 02 Investigating Information Security Events

130201 Investigating the Cause and Impact of IS Incidents

Purpose: To protect the State's technology resources by conducting proper investigations.

STANDARD

An investigation into an information security incident must identify its cause, if possible, and appraise its impact on systems and data. Agencies shall utilize trained personnel to perform investigations and shall restrict others from attempting to gather evidence on their own.

ISO 17799: 2005 References
13.2.2 Learning from information security incidents

130202 Collecting Evidence of an Information Security Breach

Purpose: To protect the State's resources through the proper collection of evidence.

STANDARD

Evidence of or relating to an information security breach shall be collected and preserved in a manner that is in accordance with State and federal requirements. The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities.

ISO 17799: 2005 References
13.2.3 Collection of evidence

130203 Recording Information Security Breaches

Purpose: To protect the State's resources through proper reporting of security breaches.

STANDARD

All information technology security breaches must be reported to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, and must include the information required on the Incident Reporting form,[2] incorporated by reference.

The agency head shall ensure that all information technology security breaches occurring within his/her agency are reported to ITS, acting on behalf of the State Chief Information Officer, within twenty-four (24) hours of a confirmed breach, as required by N.C.G.S. §147-33.113.

ISO 17799: 2005 References
13.1.1 Reporting information security incidents

130204 Responding to Information Security Incidents

Purpose: To protect the State's resources through proper response to security incidents.

STANDARD

The ITS Information Security Office, acting on behalf of the State Chief Information Officer, shall evaluate the proper response to all information security incidents reported to the agency. ITS shall work with agencies to decide what resources, including law enforcement, are required to best respond to and mitigate the incident.

ISO 17799: 2005 References
13.2.1 Responsibilities and procedures

Section 03 Corrective Activity

130301 Establishing Remedies for Information Security Breaches

Purpose: To help develop rapid resolutions to information security breaches.

STANDARD

All agencies shall maintain records of information security breaches and the remedies used for resolution as references for evaluating any future security breaches. The information shall be logged and maintained in such a location that

[2] The Incident Reporting form can be found at https://incident.its.state.nc.us/ and can be filled out online.

it cannot be altered by others. The recorded events shall be studied and reviewed regularly as a reminder of the lessons learned.

GUIDELINES

Information recorded in regard to information security breaches should cover the following areas:

- The nature of the breach and the number of systems affected.
- The services that were affected and the resources needed to implement a timely resolution.
- The time at which the breach was discovered and the time at which corrective actions were implemented.
- How the breach was detected and the immediate response after detection.
- The escalation used to resolve the breach.

ISO 17799: 2005 References
13.2.2 Learning from information security incidents

Section 04 Other Information Security Incident Issues

130401 Ensuring the Integrity of IS Incident Investigations

Purpose: To ensure integrity of electronically stored records of information systems incident investigations.

STANDARD

All agencies shall ensure the integrity of information systems incident investigations by having the records of such investigations audited by qualified individuals as determined by agency management.

ISO 17799: 2005 References
10.10.2 Monitoring system use
15.3.1 Information systems audit controls
15.3.2 Protection of information systems audit tools

130402 Analyzing IS Incidents Resulting from System Failures

Purpose: To properly analyze information security system failures.

STANDARD

Agencies shall investigate information system failures to determine whether the failure was caused by malicious activity or by some other means (i.e., hardware or software failure). Qualified technicians shall perform the investigations, which shall include:

- Checking system logs, application logs, event logs, audit trails and log files.
- Continuing to closely monitor the specified system to establish trends or patterns.
- Researching for known failures resulting from software bugs.
- Contacting appropriate third parties, such as vendor-specific technicians, for assistance.

ISO 17799: 2005 References
13.2.1 Responsibilities and procedures

130403 Breaching Confidentiality

Purpose: To develop a method for identifying and reporting breaches of confidentiality.

STANDARD

Agency staff shall report breaches of confidentiality to agency management as soon as possible.

Breaches of confidentiality include, but are not limited to, the compromise or improper disclosure of confidential information such as Social Security numbers, medical records, credit card numbers and tax data.

ISO 17799: 2005 References
6.1.5 Confidentiality agreements
6.2.3 Addressing security in third party agreements

130404 Establishing Dual Control/Segregation of Duties

Purpose: To increase the integrity of data while conducting incident investigations.

STANDARD

Agencies shall establish controls to protect data integrity and confidentiality during investigations of information security incidents. Controls shall either include dual-control procedures or segregation of duties to ensure that fraudulent activities requiring collusion do not occur.

If any suspicious activities are detected, responsible personnel within the affected agency shall be notified to ensure that proper action is taken.

ISO 17799: 2005 References
10.1.3 Segregation of duties
13.2.1 Responsibilities and procedures

130405 Using Information Security Incident Check Lists

Purpose: To report information security incidents in a consistent manner.

STANDARD

To ensure consistent reporting of information security incidents, agencies shall use the ITS Incident Reporting form[3] when reporting such incidents.

ISO 17799: 2005 References
13.2.1 Responsibilities and procedures

130406 Detecting Electronic Eavesdropping and Espionage Activities

The standard recommended by ISO 17799 in this category is not appropriate as a general standard for North Carolina executive branch agencies.

130407 Monitoring Confidentiality of Information Security Incidents

Purpose: To monitor the release of confidential information involving information security incidents.

STANDARD

Agencies shall monitor and control the release of confidential security information during the course of a security incident or investigation to ensure that only appropriate individuals have access to the information, such as law enforcement officials, legal counsel or human resources.

ISO 17799: 2005 References
13.2.1 Responsibilities and procedures

130408 Risks in System Usage

Purpose: To monitor systems usage and minimize risks.

STANDARD

System usage shall be monitored and reviewed for activities that may lead to business risks.

GUIDELINES

Items to monitor may include but not be limited to the following:

- Over utilization of bandwidth.
- Un-authorized login attempts.
- Un-authorized attempts to make changes to system settings.
- Trendy activity, such as to monitor for repeated information security attacks.

[3] The Incident Reporting form can be found at https://incident.its.state.nc.us/ and can be filled out online.

ISO 17799: 2005 References
10.10.2 Monitoring system use

130409 Reviewing System Usage

Purpose: To monitor systems usage and minimize risks.

STANDARD

System usage shall be monitored and reviewed by personnel who are able to quantify and qualify potential threats and business risks.

The reviewing of system usage shall be segregated with controls to check against monitoring personnel.

ISO 17799: 2005 References
10.10.2 Monitoring system use

HISTORY

State CIO Approval: March 22, 2006
Original Issue Date: March 22, 2006
Subsequent History:

Standard Number	Version	Date	Change/Description (Table Headings)

Old Security Policy/Standard	New Standard Numbers
Incident Management Policy	Chapter 13 – Detecting and Responding to IS Incidents
	060102 – Collecting Evidence for Cyber Crime Prosecution
	060103 – Collecting Evidence for Cyber Crime Prosecution
	060108 – Handling Hoax Virus Warnings
	060110 – Responding to Virus Incidents
	120401 – Recording Evidence of Information Security Incidents